Tab A

Preliminary Research and Development Roadmap for Protecting and Assuring the Banking and Finance Infrastructure*

* This document is one component of a longer report entitled *Preliminary Research and Development Roadmap for Protecting and Assuring Critical National Infrastructures* (Transition Office of the President's Commission on Critical Infrastructure Protection and the Critical Infrastructure Assurance Office. Washington, D.C. July 1998) For more information, please see <URL:http://www.ciao.gov/>.

Contents

Section 1 Introduction A-1

1.1 Scope of the Infrastructure A-1
1.2 Characterization of the Infrastructure A-2
1.2.1 Sophisticated and Robust Systems A-2
1.2.2 Emerging Trends A-2
1.2.3 Planning for Potential Responses A-4
1.3 Issues and Trends A-6
1.3.1 Policy Trade-offs A-6
1.3.2 New Technologies A-9
1.3.3 Internationalization of Information and Trade A-10
1.3.4 New Definitions of Value A-11

Section 2 Threats and Vulnerabilities A-13

2.1 Effects of Regulation and Control A-13
2.2 Effects of New Technologies A-14
2.3 Effects of Protecting Monetary Information A-15
2.4 Effects of the International Marketplace A-16

Section 3 R&D Topics and Activities A-17

3.1 R&D Objectives A-17
3.2 Technological Needs A-17
3.2.1 Simulation Model Development A-17
3.2.2 Information Security Analysis A-18
3.2.3 Intrusion Indication and Warning Tools A-20
3.2.4 Systems Reliability Enhancement A-22
3.2.5 Information System Standardization A-24
3.2.6 Information Security Support for Electronic Commerce A-25
3.3 Technology R&D Shortfalls A-26
3.3.1 Modeling and Simulation A-27
3.3.2 Key Management Systems A-27
3.3.3 Authentication Technologies A-27
3.3.4 Intrusion and Anomaly Detection Tools A-27
3.3.5 Computer and Network Security A-28

Contents (Cont.)

3.3.6 Physical and Electronic Protection Technologies A-28
3.3.7 Electronic Payment Systems A-28
3.3.8 Network Security Management Systems A-28
3.4 R&D Topics and Roadmaps A-29

Section 4 R&D Topic Roadmaps A-35

Section 5 References A-37

Tables

A.1 Summary of Banking and Finance R&D Topics A-30

A.2 Summary of the Banking and Finance Infrastructure R&D Roadmap A-36

Section 1
Introduction

This report examines the potential threats and vulnerabilities to the banking and finance infrastructure. In particular, various entities and systems are examined that enable the transfer of funds and monetary instruments throughout the United States and into international commerce. The purpose of this report is to present a clear and useful analysis of threats to the stability, reliability, and security of the banking and finance infrastructure. This report also prioritizes and recommends research and development (R&D) activities needed to address potential vulnerabilities.

Research and development for the banking and finance infrastructure must not only support adequate functioning of the infrastructure, but also preserve the confidence of the American public that these services are functioning. Researchers need to develop technical solutions to strengthen the overall security of our nation's financial entities and their supporting systems.

1.1 Scope of the Infrastructure

The banking and finance infrastructure consists of institutions, agencies, and support systems (physical, procedural, and data) that facilitate lending, borrowing, issuing, trading in, or caring for money, credit, and other representations of value. Included in this infrastructure are banks and credit unions; insurance companies; lending and credit institutions of all kinds; securities and commodities dealers; state, federal, and international oversight and regulatory agencies; and the web of communications equipment and linkages that support transactions among those systems. The principal stakeholders in this infrastructure are listed below:

- Federal and state governments in their roles as
  - guardians of consumer rights, protections, and responsibilities
  - issuers of legal tender and managers of the money supply
  - guarantors of national defense
  - law enforcement agencies that investigate financial crimes and illegal uses of money
  - trading partners
- Banking
- Brokerage and financial institutions
- Retail and merchant industries

- Consumers and investors
- International governments that depend on the value of the U.S. dollar
- Technology and service providers that support infrastructure security

Because of changes in the technology of, and the practices by which, the banking and finance infrastructure conducts business, it has become inexorably intertwined with the information and communications infrastructure. The primary focus of this report, however, is to look at the technical issues that affect banking and financial services. When issues are important to both infrastructures, this fact is noted, but not discussed in depth.

1.2 Characterization of the Infrastructure

1.2.1 Sophisticated and Robust Systems

The U.S. banking and finance infrastructure is the most advanced and robust system of its kind in the world. It was established to preserve the safety and stability of our financial institutions and has served our nation well. The President's Commission on Critical Infrastructure Protection has divided the banking and finance infrastructure into five sectors on the basis of the function or service that each provides. These sectors are banks, non-bank financial service companies, payment systems, investment companies and mutual funds, and securities and commodity exchanges.

1.2.2 Emerging Trends

In comparison with other nations, the United States has a long history of safe and sound banking and financial services. Occasional crises have occurred because of structural imbalances, which were corrected by subsequent legislative and administrative initiatives. However, the banking and finance infrastructure is now at its most potentially chaotic time since the 1930s. Four trends have caused this unrest: (1) deregulation and increased competition, (2) convergence of technologies, (3) internationalization of commerce, and (4) changing definitions of value. These trends are discussed in the following subsections.

Deregulation and Increased Competition

The first driving force in the development of financial services is the movement toward deregulation of the industry. Deregulation has created competitive pressures at every level, as banks, insurers, security and commodity brokers, and issuers of credit search for ways to capitalize on this new freedom to compete with one another. As competition intensifies, margins narrow and risk assessment, on the part of both producers and consumers of financial products and services, becomes more challenging. Another issue is how to determine which entities must be regulated. If, for example,

providers of technology and communications services begin to offer financial and banking services, old regulatory paradigms may not be relevant or applicable.

Convergence of Technologies

The second trend consists of (1) the convergence of computer, video, and telecommunications technologies and (2) the increasingly rapid pace at which new technologies are being introduced into the industry. In particular, three technologies are transforming the way in which the banking and finance infrastructure conducts its business:

- Ubiquitous digital broadband links with superfast switching;
- Advanced digital television, desktop video, and high-resolution imaging; and
- Wireless and mobile communications.

These new technologies, which were embryonic a few years ago, present new challenges to those persons involved with banking and financial services. Both those who compete in the nearly limitless marketplace and those who struggle to guide and protect the individuals participating in that marketplace now must contend with these new modes and means of transactions.

Internationalization of Commerce

A third trend also affects the industry. International borders, which were once an effective barrier to financial fraud or persons with malevolent intent, are no longer a deterrent. Today's marketplace is global in time and space: money moves around the world and from time zone to time zone at the "click of a mouse." A single nation with a regulatory and/or law enforcement establishment cannot cope in isolation with the volume and speed of transactions.

Changing Definitions of Value

Finally, the nature of what is being traded in this new virtual marketplace is changing, and its ultimate form is unknown. Walter Wriston said, "Today, information about money is more valuable than money itself" (Wriston 1992). Knowledge about how value is represented, stored, and exchanged is, in itself, a potential new form of wealth. Because this knowledge has value, it becomes a target for theft. It must be protected, as it is stored, moved, and traded.

The potential effects of these forces must be identified, and plans must be made to implement recovery actions. If these actions are not taken, the banking and finance infrastructure, which is a high-reliability/low-consequence system that conducts millions of nearly error-free operations daily with little risk of catastrophic consequences, could

change to a lower-reliability/higher-consequence system that has more frequent errors and greater penalties for failure.

Compared with the other infrastructures that support our nation, the banking and finance infrastructure is well protected to withstand all but a full-scale, national-level attack. This protection is the result of our nation's investment in security, which has been fundamental to the development and management of the banking and finance infrastructure for several reasons:

- Accountability and oversight up to the board level;
- Security that is integral to risk management; and
- Major investments in security, diversity, backup and recovery, and policies and legislation, which provide the law enforcement framework for protecting both national security and private interests.

Changes to the banking and finance infrastructure over time have included significant investments in leading-edge technologies. These investments have been made separately by the federal government and private industry and by collaborative efforts between the two. The result has been increased security and a reduction of known and perceived risk in the infrastructure. The federal government, for example, recently issued new $100 bills to provide an additional deterrent to counterfeiting. New bills in other denominations will follow soon. Similarly, private industry has invested in and implemented Cardholder Authentication Verification technologies to thwart attempts to present counterfeit magnetic stripe cards for interacting with the banking and finance infrastructure. For example, financial institutions have added photos and holograms to cards to improve authentication of electronic representations of value (e.g., MONDEX). These institutions were quick to adopt network miniservers and personal computers and are considering the move from magnetic stripe to smartcard technology, which will increase their ability to secure transactions and provide stronger distributed authentication.

1.2.3 Planning for Potential Responses

It is important to consider how the security investments cited in the preceding subsection are justified.

> Industry views security investments as a necessary cost of doing business, to ensure the availability, integrity, and confidentiality of their data.… Financial institutions manage risk against known and perceived threats. When the industry becomes aware of new threats or vulnerabilities, firms will quickly move to address the problem.… However, in developing their security posture, most network owners and operators do not plan to defend against a structured, deliberate attack or a subtle, non-criminally

> motivated, confidence-level attack using advanced information warfare tools and techniques. Rather, these firms focus on preventing failures resulting from natural disasters (floods, hurricanes) or preventing financially motivated criminals (not only outsiders but also insiders) from defrauding their business. In short, due to a lack of a business case or data for their risk management models, organizations are not implementing national-security-level protective measures. Rather, they protect business systems from hackers and criminals, who they perceive as the most likely and most damaging threats.…Industry currently does not have reliable access to consistent sources of current and accurate vulnerability, threat, and capabilities data to 'feed' into its risk models. Furthermore, there are limited mechanisms for sharing data within, or across industries for assessing systemic vulnerabilities (Booz-Allen and Hamilton, 1996).

Many participants in the banking and finance infrastructure have instituted reliable threat models and mitigation measures that can dramatically reduce the effect of an attack, short of a state-sponsored act of war. The efficacy of these tools depends, however, on having appropriate, accurate, and timely information, including that collected by the U.S. government and international agencies.

Both government and industry need reliable, common access to current and accurate data on vulnerabilities, threats, and capabilities. These data can be "fed" into risk models that will provide information to help ensure continual protection of the infrastructure. Industry and government associations and agencies are being formed to identify requirements and institute processes for sharing information. Examples of such groups are the Federal Agencies United against Fraud, which sponsors the Fraud in Cyberspace Conference, and the Financial Services Technology Consortium.

Few mechanisms, however, are available for sharing relevant data that are not related to law enforcement. Information sharing is critical if today's threat models are to be expanded to defend the infrastructure against terrorist and nation-state attacks. Sharing a broad range of information requires innovative methods to protect the rights of those to whom the information pertains and the exposure of those who provide and use the information. Legal concepts, such as use immunity and statutes of repose from liability, may need to be assessed to determine their applicability and possible implementation.

At this time, government and industry investments in advanced technologies are not sufficiently coordinated to guard against potential terrorist and nation-state attacks — the greatest potential risk to our nation's banking and finance infrastructure. Consider, for example, information system technologies, including distributed network management (improves efficiency and reliability of service), cryptography (secures automated transmissions of monetary value and authenticates the participants in any given transaction), and pattern recognition algorithms (detect indications of fraudulent behaviors). While both our government and industry have invested in R&D for these key technical areas, only ad-hoc mechanisms are available for sharing the results of these

investments. As the network of systems underlying this infrastructure becomes more complex, it is critical to coordinate research aimed at coping with the vulnerabilities inherent in that complexity.

1.3 Issues and Trends

1.3.1 Policy Trade-offs

Regulation and Control

The U.S. banking and finance infrastructure is a centrally controlled system backed by the federal government since the 1860s. Since that time, the U.S. Treasury has tightly controlled the representation of money or economic value. Changes in the way that our nation issues coins and currency have been made during the twentieth century to protect against counterfeiting, thereby reducing risks inherent in the infrastructure. Although the policy and legislative guidelines have remained the same, there is a significant precedent for protecting both the interests of the nation as a whole and the interests of our citizens as individuals. Consequently, the behavioral environment for exchanging money for goods and services has had a defined framework within which individuals operate. Modes for spending or exchanging money, investing money, moving money, and communicating the way in which money is moved between exchange entities are based on trust models that are understood by those involved in economic exchange processes.

The purpose of regulating banking and finance in the United States is to maintain the surety, or security, of the system. For banks, regulators have adopted rules based on generally accepted performance indicators:

- Capital adequacy,
- Asset quality,
- Management competency,
- Earnings, and
- Liquidity.

For the investment side, statutes, case law, and regulatory practice have resulted in a standard that balances the protection of investors from fraud and deceit and the promotion of free exchange of value among ready, willing, and able buyers and sellers. The underlying principle is full disclosure of information necessary to facilitate an informed exchange of value. Regulators cannot set the exchange rate for representations of value; investors or purchasers must make that decision. Regulators can only act to ensure that relevant facts are not intentionally withheld from buyers and sellers. This

balance between supporting the market and protecting participants has been maintained by focusing on the following elements of financial services:

- *Products* — Most representations of value offered to the public must be registered with federal agencies, state agencies, or both.

- *Practices* — Regulators have attempted to prevent persons with fiduciary or insider status from offering misleading or false inducements or from manipulating buyers and sellers of financial products.

- *Prices* — Regulations set up to limit excessive or inflated pricing of specific representations of value establish limits on interest rates, service fees, and other transaction costs. These rules are intended to ensure that the price paid for any representation of value accurately reflects the true, underlying value of that instrument.

Both managers and regulators of the banking and finance infrastructure are striving to balance four competing goals: security of entrusted value, growth and adaptation of new opportunities, competitiveness in the market, and flexibility to meet uncertainty. The difficulty is that not all financial institutions respond equally to uncertainty or to adaptation of new technologies and products. Likewise, not all regulators are equally able to recognize when a single goal is being overemphasized to the detriment of others. Moreover, not all institutions are subject to the same level of regulation.

The banking and finance infrastructure has an enormous stake in maintaining the trust and confidence of the public in the stability and safety of financial services and products. Members of the industry must balance the severity of a risk against the costs of mitigation. The infrastructure regularly stresses this tenet of operation. Banking, in particular, has developed many techniques and tools to assist managers in analyzing systemic risk. Today, however, the entire infrastructure is constantly under pressure to become more competitive in a continuously shifting marketplace in which the old rules may not apply.

An increasing problem for both industry and regulators is that this new, super-competitive electronic marketplace has little relationship to the location or origin of their products and services. More and more, they are acquiring operational services (e.g., software development, contingency data storage, data processing, communications linkages) needed to support this spatially and temporally disaggregated marketplace from outside sources not directly subject to the standards of the industry. Added to the impact of the electronic marketplace is the industry's response to regulatory pressures to increase competition. To maximize their rate of return, many firms in the industry have concentrated their assets and operations and also reduced their overall workforce. Taking these measures has created more lucrative targets for criminals and generated dissatisfaction among displaced workers, which constitutes an additional threat.

The industry wants the freedom to adopt or exploit opportunities in the new marketplace, but it does not want to be divided by the forces discussed above. Industry leaders want to have a strong voice in shaping whatever regulatory structure is developed to address the new issues in the emerging industry. Of primary concern is that industry leaders do not want to be forced into taking risks that are poorly understood and poorly defined. They would prefer to wait for a regulatory definition, while Congress and the regulators respond to a public demand to "do something."

Regulatory practices can significantly affect the safety and security of the banking and finance infrastructure in terms of balancing economic risks and opportunities. The effects of regulations that would protect the industry as a national infrastructure (that is, in the sense of protecting the industry from intentional ill will) are unknown. However, it is clear that forces shaping the new structure and movement of the industry are already being felt and that to provide significant help, regulatory structure and practices must become more flexible and adaptable.

The banking and finance infrastructure has implemented various security measures and safeguards to protect assets and respond to regulatory pressure. Currently, protecting this infrastructure is affected more directly by regulations established for the information and communications infrastructure. However, changes are expected in the future. Appropriate protective measures may depend on the type of threat, although some measures may be common to all threats. Threats to the banking and finance infrastructure can be categorized as follows:

- *Physical theft or destruction*. Terrorists could attempt to incite financial panic by stealing physical assets or destroying financial data banks or the communication systems that support transactions so that they cannot be used. This type of threat could involve either physical (e.g., bombing a key facility) or cyber attack.

- *Corruption or destruction of data*. Criminals or terrorists could attempt to corrupt or delete information in key systems. For example, they could try to disrupt banking, commerce, or utilities by "hacking" into particular systems. They could then either input false or misleading data, delete data, or deliberately manipulate the system (e.g., "zero out" or increase a bank balance).

- *Unauthorized access to information*. Criminals or others conducting national or industrial espionage could attempt to use information systems to obtain proprietary data or "private" information (in the personal sense).

The greatest damage from any of these threats (physical or cyber) is outright denial of service. The most harmful kinds of attacks against the infrastructure are those that cause the public to perceive the system as unreliable, leading to a serious lack of confidence in the system. Regulatory structure and practice must directly help to define products, practices, and prices in this emerging new structure. To meet this obligation, regulators

require new tools with which to assist the industry in defining risk, assessing threats, and responding to crises.

National Security and Promotion of Commerce

A national debate is under way concerning the balance between using technologies to ensure the national defense and to support international competitiveness. Central to this debate for the banking and finance infrastructure are our nation's cryptographic policies. This debate must be resolved before public key systems can be deployed on an international basis with adequate security to protect the assets of the banking and finance infrastructure.

1.3.2 New Technologies

The extent of the interdependence between the information and communications infrastructure and the banking and finance infrastructure is now so significant that it is difficult to conceive how modern banking and finance could be carried out without full and reliable access to a secure telecommunications system. Increasingly, the access to and reliability of that system depend on the same crucial communications and computing technologies. This combination is collectively referred to as the National Information Infrastructure (NII). One group of experts has characterized the importance of the NII to banking and finance in this way:

> Much of the way money is accounted for, handled, and exchanged is now done via the NII. Salaries are directly deposited into bank accounts by electronic funds transfers. Automated teller machines … deposit funds, withdraw funds, and make payments. When payment is made for merchandise with debit cards and credit cards, transactions are verified using the public switched [telephone] network. Much of our national economy also depends on the NII. The vast majority of transactions conducted by banks and other financial institutions are done via electronic funds transfers. Over $2 trillion is sent by international wire transfers every day. In addition, most securities transactions are conducted via computerized systems (U.S. Senate 1996).

In the next decade, six trends in technology are probably going to dramatically alter the banking and finance infrastructure:

- Convergence of communicating, computing, and imaging into integrated platforms;
- Proliferation of networks using asynchronous transfer mode cell switching to integrate voice, data, and video for transmission among users;
- Increased reliance on digital communications;

- Increased use of digital signatures for executing agreements;

- Improvements in pattern-directed inference systems for detecting potentially fraudulent or otherwise illegal activities on networks; and

- Deployment of packet-switching protocols throughout the communications and computations networks that support the industry.

The positive effects of these trends on the banking and finance infrastructure are likely to be increased speed, convenience, and openness for all participants. The negative effect is the potential for increased vulnerability to misuse of the systems that comprise the industry's supporting infrastructure. Increased vulnerability could result from more openness, without commensurate attention to security, and disparate rates of introducing new technologies among the many participating institutions and entities. For example, older, slower systems could be overwhelmed by faster, information-dense systems. One expert has defined the issues somewhat differently, but not inconsistently:

> New technology, which includes faster switches, higher speed routers, etc., is being developed, but technology takes time. In the security area, faster encryption algorithms, electronic signatures, cyber notaries, and data compression algorithms need to be developed to send more data in less time while providing secure, confidential, and authenticated network links.
>
> The Internet is technically capable of growing almost infinitely. The major constrictor of growth will be how the user communities will deal with securing intellectual property rights, the security of transactions, and other sociological issues (Kennedy 1998).

The challenge is to ensure that technologies introduced to enhance performance of the infrastructure do not unintentionally reduce the security of the infrastructure.

1.3.3 Internationalization of Information and Trade

The effect of new technologies (e.g., Internet connectivity and the size of the asset pool that is electronically connected worldwide) is significant in many ways. Does greater connectivity motivate criminals to attempt to defraud financial institutions and systems? Furthermore, does greater connectivity lower the risk of exposure because of the potential to remain anonymous over open public networks (e.g., the Internet)? Also, the latest changes in technology allow foreign nation-states to "leapfrog" implementing infrastructure (e.g., investing in pervasive communications systems) by moving to technologies that support electronic commerce, such as the smartcard, cellular phone and satellite communications, and cryptography.

The United States must embrace electronic commerce to participate in international economic exchanges. New technologies are changing the definition of

"money" and presenting an incentive for moving toward nontraditional representations of money, such as electronic money (or E-money) and stored-value cards issued with or without bank involvement. Growth and expansion within this infrastructure are primarily based outside the United States and come at a time when both government and private-sector investments in R&D funding are more limited and in need of reassessment. Decentralization of operations over multiple platforms (rather than being concentrated on a single mainframe with backup capability) makes information at greater risk from tampering, theft, or misuse at any single point.

1.3.4 New Definitions of Value

Efficient commerce depends on well-understood, highly trustworthy definitions of value, financial obligation, money, and legal tender. Value is the underlying utility of an object, for example, weighted by its cost. Just as so many pounds of potatoes are "worth" so many units of money, a given quantity of ownership or control of a financial obligation or expression of ownership (e.g., stocks, bonds, notes, or evidence of debt or guarantee of payment) is also worth so much in exchange.

Money can be any generally accepted medium of exchange or unit of account. A unit of money can represent a certain fixed quantity of a physical substance (e.g., gold, silver, platinum, or potatoes), or it can represent an expectation of value relative to other media of exchange.

The U.S. dollar has value far beyond the intrinsic utility of the paper on which it is printed because, as legal tender (e.g., coins and currency issued by the federal government), it is backed by the full faith in, and credit of, the nation.

Until recently, these relationships among value, financial obligation, money, and legal tender have been clearly defined in the United States because of four stabilizing factors:

- Tightly controlled processes of coinage and issuance of currency;
- Secure and robust communications infrastructures;
- Well-defined authentication practices; and
- Recognizable forms of exchange with known guaranteed exchange values.

Traditionally, the industry has had a clear understanding of the assets within the infrastructure that require protection (Wriston 1992):

> . . .[Technological] developments, generally referred to as the information revolution, are causing a shift in the balance of economic, political, and military power and are changing relationships among government,

> citizens, and private institutions. Two technological advances — communications technology for transmitting information and modern computer systems for processing data — are driving many of these changes. . . . The systems built around these technologies and the information they process, are now key to delivering the goods and services of the nation. Today, lights would go out, airplanes would stop flying, and financial institutions would shut down if the supporting computer systems and networks ceased to function. As these changes have evolved, information has become the "capital" for the future; causing a shift in perspective as to the assets that need protection.

We have entered an era in which these traditional relationships among value, financial obligation, money, and legal tender can become unstable because three of the four stabilizing factors are undergoing major changes. The one relatively stable factor — the federal government's minting of coins and issuance of currency — will also have to be adapted to accommodate the new realities.

Section 2
Threats and Vulnerabilities

2.1 Effects of Regulation and Control

The architecture and dynamics of the banking and finance infrastructure are not comprehensively understood. Some components of the systems are static, "stovepiped" items. Discrete functionalities, protocols, and practices are studied independent of the systems into which they are embedded. Regulatory practices and processes are often viewed as hindrances to the efficiency of the marketplace, but can, in fact, add to the confidence and efficiency of the system and contribute to infrastructure assurance.

Because no comprehensive model of the banking and finance infrastructure exists, the impacts of regulatory agencies on this infrastructure are not easily studied. Several issues have become apparent, however. They are listed below along with recommendations to address them.

Issue 1. The lines between federal and state regulatory practices and structures must be as transparent as the lines among local, state, national, and international commerce in financial products and services. It will be necessary to rethink the balance between supervisory and regulatory approaches to practice and the intentional assignment of oversight responsibility to the level closest to where commerce is being conducted.

Recommendation 1. Research should be conducted to define the appropriate structure of oversight agencies for the emerging banking and finance infrastructure at the local, state, federal, and international levels.

Issue 2. More immediate response to problems is needed. Regulators and examiners should begin to monitor the activities of the infrastructure by observing operations in real time, rather than depending on periodic reports generated after the fact.

Recommendation 2. Research should be performed to determine how stakeholders could conduct on-line supervision and oversight. This research should include such techniques as pattern recognition, expert systems, and risk-assessment tools available on-line to both the industry and regulators, so that perceived problems can be recognized and corrected immediately.

Issue 3. Examiners need to have timely and economical training and continuous education. This need should increase as the pace of changes in the industry

accelerates. New tools, and the nature of the evolving infrastructure that requires these tools, are complex and unfamiliar to most examiners and regulators.

Recommendation 3. R&D should be conducted to examine distance learning capabilities and on-line expert systems to help to prepare and train examiners and regulators.

Issue 4. The definitions of products, practices, and prices in the industry need to be standardized among state, federal, and international statutes and regulations. All parties involved need to understand what is being regulated, especially because billions of transactions occur in cyberspace 24 hours a day.

Recommendation 4. R&D in model law should be undertaken to clarify regulatory subjects in the emerging infrastructure and standardize the laws and regulations among agencies and between levels of government.

2.2 Effects of New Technologies

The U.S. Department of the Treasury has stated that "[n]ew technology and new ways of using current technology is [sic] making it possible to manage, perform, and create in an environment of shared resources and shared power" (U.S. Department of the Treasury 1993).

While these technologies make financial transactions more efficient, they also make it more difficult to secure the support systems. Each additional point-of-presence in the network of systems and persons in the banking and finance infrastructure creates an additional potential for electronic tampering or attack. The General Accounting Office (GAO) (1996) has stated:

> These advances promise to streamline…operations and improve delivery of…services. However, they also increase the potential risks that sensitive and critical information could be inappropriately modified, disclosed, or destroyed, possibly resulting in significant interruptions of service, monetary losses, and a loss of confidence in the...ability to protect confidential data on individuals.

The efficiency, flexibility, and adaptability that make these new technologies so attractive to the banking and finance infrastructure also create subtle, but potentially catastrophic, weaknesses in the systems. Computerized systems "empower users to perform their jobs more effectively" (Jones and Sicherman 1997). The nexus of communications, computing, and imagery technologies makes it possible, however, for every point-of-presence to have a *custom* approach in interfacing with a network. The flexibility and adaptability create significant problems in attaining desirable states of security for that network, other networks with which it interacts, and the data being handled.

2.3 Effects of Protecting Monetary Information

The GAO (1996) report discusses the vulnerability of government systems, but the warning about vulnerability also is valid for systems that support the banking and finance infrastructure. In addition, this report continues with a statement that parallels the concerns voiced by banking systems experts during Commission interviews; that is,

> …the potential risks are increasing because automated systems and records are fast replacing manual procedures and paper documents, which in many cases are no longer available as 'backup' if automated systems should fail. These vulnerabilities are exacerbated because, when systems are interconnected to form networks or are accessible through public telecommunications systems, they are much more vulnerable to anonymous intrusions from remote locations (1996).

The common response to dealing with increased vulnerabilities is to improve encryption, especially for those vulnerabilities that arise from the combined effects of (1) more individual points of presence in a network, (2) faster processors and nearly unlimited storage memory, and (3) greater on-line access to more detailed data. Encryption has been applied in two venues: protection of data and "cloaking" of transactions. The government has invested in extensive research into creating and maintaining cryptographic systems to satisfy the needs of the banking and finance infrastructure. The release of some useful technologies for commercial use has been deterred, however, because the government is required to keep "master keys" for all encryption systems. This requirement is based on law enforcement and national security issues. All security applications are subject to the same vulnerability as systems that provide a "back door" to satisfy this government policy — the concern merely shifts from security of the data and transactions to the security of the master keys. In addition, it is not clear how international companies may react to U.S. policies about key repositories and types of encryption.

The banking and finance infrastructure is becoming more enmeshed with communications technology, which creates an additional security problem. The former has been slower to totally replace physical records and manual procedures and processes than have some of the other service industries. Although the industry is, therefore, relatively more able to respond to system failure, this positive aspect is somewhat offset because of a continued reliance on the integrity of key individuals to authorize and validate certain actions. As a result, the banking and finance infrastructure does not have the advantages of automated audit tracking and surveillance tools. However, such tools cannot replace, but only supplement, trusted employees who operate under dual control systems with stringent audit mechanisms.

2.4 Effects of the International Marketplace

The United States has been the world leader in the "information revolution," which began in 1946 with the invention of the first computer. Since that time, much of our nation's infrastructure has depended on reliable, secure operation of information systems to preserve and protect national welfare and interests.

However, the information revolution is no longer contained within the United States. Persons involved in the banking and finance infrastructure need to recognize the effects of communications technological developments on the international marketplace:

> The globalization of information technology has posed the potential threat of information weapons, which could be one of the most effective, cheapest, and simplest avenues for terrorists and/or nation-states to deploy in order to cripple U.S. defenses. These weapons have been described as great equalizers that help small nations against larger nations. Information warfare attacks could conceivably be conducted with relative anonymity from anywhere in the world (Defense Science Board 1996).
>
> …It would be naive to believe that other nation-states, and probably terrorist organizations, are not developing [information warfare tools].… However, lacking credible evidence of existing information warfare attacks on the United States or a physical attack specifically targeting electronic systems, it is unlikely that industry will plan to defend itself from terrorist and nation-state attacks (Booz-Allen and Hamilton 1996).

Section 3
R&D Topics and Activities

3.1 R&D Objectives

The banking and finance infrastructure must preserve the public's confidence in the nation's economy. Management and control of the value of the U.S. dollar are key to the continued confidence of both consumers and international trading partners. National security is, by definition, an underlying goal of this R&D effort.

3.2 Technological Needs

3.2.1 Simulation Model Development

Description

Industry policy makers and planners do not clearly understand the potential impacts and interdependencies of the forces behind the rapid changes within the banking and finance infrastructure. The infrastructure is so diverse that a simple characterization cannot adequately express the potentially complex results from either public or private initiatives that affect components of the infrastructure. Considerable effort is needed to develop a constructive strategic simulation model of this infrastructure. As the model is developed, maintained, and elaborated, analysts can develop increasingly effective strategies that can be used to examine (1) policies and requirements for managing the infrastructure and (2) mechanisms for responding to threats to that infrastructure.

Goals and Challenges

The model must be able to simulate both the technical reactions of the support systems and the probable public and industry reactions to regulatory initiatives and information dissemination initiatives. Other characteristics of the infrastructure also should be modeled. For example, the National Infrastructure Protection Center, which was recently established within the Federal Bureau of Investigation, could use such a model to advise industry on the potential effects of proposed technologies (Reno 1998). This function would require sensitivity in managing and controlling information.

Rationale for the Research and Desired Results

Only a constructive model that can serve as the basis of nondeterministic simulations of the banking and finance infrastructure can satisfy the requirements of the

various stakeholders. Such a model, made available through a national user facility, would enable stakeholders to:

- Develop new business risk models;
- Examine the effects of policy trade-offs, shifts in technology, the international marketplace, and various open market standards;
- Validate oversight and training programs;
- Validate intrusion indication and warning tools; and
- Validate system reliability under alternative scenarios, while ensuring that consistent internal logic is used throughout such an analysis.

Timeframe and Resource Requirements

In the near term (before 2002), researchers would engage industry to develop a constructive strategic simulation model (CSSM). Funding required for these efforts is estimated to be $18 million. Before 2005, research activities would include development of the requirements, legal basis, policies, and techniques for protecting data for the CSSM. Funding required for these efforts is estimated to be $10 million. Before 2010, researchers would prepare a field operational model and life-cycle management plan. The cost for this work is estimated to be $1 million.

3.2.2 Information Security Analysis

This topic includes cryptographic research and entity authentication.

Description

Today's approaches for implementing cryptography balance the issues of anonymity and nonrepudiation. Protection of privacy in transactions needs to be balanced with the requirement to be certain of the identities of the parties involved. It needs to be decided whether it is important to maintain an audit (paper) trail to provide evidence of economic transactions (i.e., nonrepudiation) to a third party (someone not involved in the economic exchange). This procedure would support private rights, meet legal requirements for financial reporting, and help to resolve financial electronic crimes.

If it is determined that an audit trail is of paramount importance, secondary or less importance can be placed on anonymity. In a paper cash system, anonymity in the transaction is possible. Persons pay in cash for goods and services without proving their identities. If paying cash is of paramount importance to an E-money-based economy, nonrepudiation must be less important. Certainly a trade-off is inevitable between

anonymity and nonrepudiation. Research needs to be conducted to determine the best ways to support both interests simultaneously.

Goals and Challenges

Cryptography allows party A to send information to party B across open public networks or communications channels. It gives a defined level of confidence that the data received by party B actually came from party A and not from someone masquerading as party A. It also ensures that the information received has not been altered during transmission and that another party has not substituted a false message for a legitimate one. Most important, by applying an encryption algorithm, cryptography ensures that intruders or unauthorized parties cannot read the message.

Issues that arise in the management of public keys, which are used for encryption purposes, can become onerous. Research is needed to study, develop, pilot test, and investigate the liabilities associated with public key infrastructures to enable secure electronic commerce. Financial standards are in place in this area; however, they need to be assessed before being applied in the future secure financial environment.

"Entity authentication" refers to a person or an organization (e.g., bank or merchant); it also refers to authentication of a device as a deterrent to counterfeit smartcards, cash, or tokens of any kind required to confirm a person's identity. Authentication is best provided by presenting three types of personal signatures in an integrated architecture: (1) informational, something that you know (e.g., a personal identification number [PIN] or a password); (2) credential, something that you have in your possession (e.g., a card, key, or badge); and (3) biometric, something that you are (e.g., fingerprints, DNA, or other bio-physical characteristics unique to an individual). The authentication system should require simultaneous presentation of all three signatures.

Research is needed to reduce ambiguity in these measures and to ensure that an unauthorized person cannot take another person's property. Research in authentication is key to the future of the banking and finance infrastructure because of the lack of personal relationships with clientele, especially when trading partners are geographically distant, which is common in international electronic commerce. Research also is needed to prevent persons from manipulating the system to discover combinations of specific data (see numbered items above) about an entity that can compromise authentication.

Rationale for the Research and Desired Results

Scalable public key management systems are necessary to address top-priority management issues posed by the broad reach of principal players in the banking and finance infrastructure. Some entities have to be trusted to manage keys (e.g., key generation, key storage, key delivery), and trust can be a difficult problem in international systems.

Some entity or group of entities must be responsible for validating private or public key pair holders and certifying electronic identities. These certificates can expire or be revoked. This entity often is referred to as the "certificate authority." Very large, scalable systems could require multiple certificate authorities in a network. How will users certified by one certificate authority trust users certified by another certificate authority (i.e., cross-certification issues)? Interoperability issues must be addressed in international environments. They are difficult problems, not only technically, but also politically. National interests and interest in international competitiveness and interoperability must somehow be reconciled to support, if not facilitate, international economic exchanges.

If the banking and finance infrastructure is characterized by E-money systems and nonstandard representations of money, by both banks and non-banks, how will recipients of electronic commerce messages verify the integrity and originator of these messages? Authorization is an important function in the banking system, so the meaning of identity certificates needs to be understood, and the use of other types of certificates (e.g., attribute or capability certificates for authorization) needs to be researched and pilot tested.

The enormous trust placed in information systems mandates far more security than is currently in place. R&D is needed for key management, cryptographic functions, key generation, and storage and manipulation of fungibles (e.g., items capable of mutual substitution; they are interchangeable). More secure computer hardware and software, and capabilities in operating systems, networking, and operations, need to be developed. Without such advances, cryptography will fail to meet the needs identified.

Timeframe and Resource Requirements

In the near term (before 2002), research would focus on developing a legal and procedural basis for expediting access to government off-the-shelf cryptographic analysis and surety analysis technology. Security standards would be developed and validated, and the efficacy of implementing cryptographic and surety technologies would be analyzed. Funding required for these efforts is estimated to be $32 million. Before 2005, research would focus on implementing a balance in anonymity and fielding scalable key public management systems. Funding required for these efforts is estimated to be $6 million. Before 2010, researchers would field entity authentication technologies. The cost for this work is estimated to be $1 million.

3.2.3 Intrusion Indication and Warning Tools

Description

The current banking and finance infrastructure is capable of indicating problems and issuing warnings based on physical attributes and documented evidence. For example, these attributes and evidence imbalances alert security teams, who then review

physical evidence and electronic indicators and begin corrective measures (as needed). People monitor the integrity of sections of the infrastructure and provide warnings and indications of problems. The borders of our nation and the redundancy of systems that must integrate to verify operational integrity (e.g., output from information systems, paper reconciliation processes, telecommunications confirmations and authorizations) are helpful in this process. The federal government monitors the economy and makes adjustments and modifications to control inflation on the basis of similar mechanisms and indicators, but on an international level.

Goals and Challenges

Changes in the banking and finance infrastructure have resulted from (1) emerging technologies (e.g., network connectivity, satellite communications, new forms of monetary value) and (2) new entries to the competitive marketplace both nationally and internationally (e.g., the insurance industry and non-bank providers of bank cards). These changes preclude the need for, and the effectiveness of, many of the physical control processes that the infrastructure depends on for assurance of faithful execution. Total dependence on information systems data for indications and warnings is a possible solution; however, it requires a more careful look at security, integrity, authentication, reliability, and availability. Other solutions for redundant indicator paths need to be evaluated and instituted, not only at the industry level, but also at the national and international levels.

Rationale for the Research and Desired Results

The United States needs to plan for the security of the banking and finance infrastructure to protect our national interests and ensure public confidence in an international electronic commerce exchange environment. To design and operate such a framework, evaluators need to assess vulnerabilities and threats on a regular basis so that prudent risk management mechanisms can be implemented. Furthermore, the government needs to know when a nation-state or a terrorist attack causes discrepancies in the infrastructure. This information is valuable in terms of supporting not only our national defense, but also retaliation, as appropriate. Infrastructure principals also need to know when natural disasters or operational errors cause discrepancies so that they can deal appropriately with public reaction. Part of this effort should include research into ways of dealing with disseminating information to the public; in addition, panic management planning should be a part of this effort.

For the government to protect our nation by means of financial crime prevention and law enforcement, the operations of the Financial Crime Enforcement Network (FinCEN) and the Secret Service Financial Crimes Division must be redefined. These agencies focus on combating money laundering and counterfeiting, respectively, but currently are not specifically authorized to protect our infrastructure. Their internal processes and controls are based on the physical borders and boundaries that provide for checks and balances within the system. Given that physical boundaries do not exist in

cyberspace, their primary functions need to be reexamined for the benefit of the country. Our new environment has generated a need for tools to assess national vulnerability and threats; these tools also support the design of threat mitigation techniques that can be used not only by FinCEN and the Secret Service, but also by industry security teams and services.

Timeframe and Resource Requirements

In the near term (before 2002), research would focus on using insight gained from work on the CSSM to determine where sensitivity tools and techniques within I&W are applicable. Researchers also would determine what data are required to implement those tools. Funding required for these efforts is estimated to be $9 million. Before 2005, research would focus on development of an initial set of tools. Funding required for this timeframe is estimated to be $7 million. Before 2010, researchers would field all operational tools. Funding required for this effort is estimated to be $1 million.

3.2.4 Systems Reliability Enhancement

Description

Research into issues that affect the reliability and recoverability of the banking and finance infrastructure should produce the following:

- "Reliability-increasing" techniques for continuing transactions through interruptions;
- Alternative routes, tools, and techniques for dealing with interruptions;
- Alternative routes, tools, and techniques for seeking alternative routes;
- New methods for recording the state of transactions;
- Automatic detection of attempts to overload the system and automatic healing around these attempts;
- Capabilities for detecting new ways to commit fraud or defeat the system and for adapting continuously with new defenses;
- Operations in the event of compromise (e.g., a root certificate);
- Operations in the presence of a communications outage; and
- Degraded mode operations.

The critical functions of secure systems typically operate on a trusted computer system to ensure that the authority for degradation can be validated. Technologies that should be explored as tools to deal with system reliability issues include the following:

- Design and deployment of dynamically configurable firewalls to protect against specific attacks while allowing authenticated transactions to continue;

- Network agents or "benign viruses," which are used for data aggregation (studied from both an offensive and a defensive perspective to support infrastructure surety); and

- Information systems that "heal" themselves or can be designed to facilitate recovery.

Goals and Challenges

Technology evaluations and integration surety issues need to be studied, and recommendations need to be made available to managers of the infrastructure. Effective analysis of these issues must be based on the constructive simulation model. A "trusted computer system" needs to be mapped to incorporate "a trusted computer network" in support of the banking and finance infrastructure. Accomplishing this mapping — and understanding its implications — requires significant effort because of the complexity and interdependencies involved. Effective and timely analysis is nearly impossible if a constructive simulation model is not available.

Rationale for the Research and Desired Results

Trusted systems traditionally have provided the basic capability for computer systems that have ultra-high requirements for availability and reliability. Trusted systems have been accredited to perform their required tasks in the presence of failures. Failures can be manifested in several ways: intrusion by unauthorized users, design errors, or the erroneous functioning of a component.

A current trend in the design of computer-based information systems for application in critical systems is to construct a reliable system from unreliable parts. Providing secure methods for transferring information over open public networks is critical for the banking and finance infrastructure because it must maintain the trust of its customers. Because open public networks are not secure, research must be increased to develop and implement new design techniques. These systems use redundancy, layering, and diversity paradigms to detect failures in a hierarchy and gracefully degrade to a state that provides a less functional, yet more trusted, configuration for operation.

Timeframe and Resource Requirements

In the near term (before 2002), research would focus on developing, publishing, and initiating implementation of standards and specifications. The focus would then turn

to developing prototypes of network security agents. Funding required for these efforts is estimated to be $54 million. Before 2005, researchers would complete implementing the standards and specifications, as well as the prototypes of network security agents. Funding required for these efforts is estimated to be $15 million. Before 2010, the prototypes of self-healing systems, configurable firewalls, and network security agents would be "fielded." Funding required for these activities is estimated to be $2 million.

3.2.5 Information System Standardization

Description

Because new employees, customers, and other individuals; products; and technologies are introduced regularly into the banking and finance infrastructure, the industry and its regulators need to establish new standards for defining risk, assessing threats, and specifying required responses to crises. These standards must result from a collaborative effort and be administered in the same way. New organizational designs must be conceived for overseeing the infrastructure. These designs must effectively allocate responsibilities and authority among federal and state agencies, international treaty organizations, and industry associations. All standards and organizational templates must be as open and flexible as possible to accommodate the rapid changes and increased complexities, which are characteristic of this industry.

Goals and Challenges

Currently, elected officials — particularly members of Congress — and regulators are struggling to agree on ways to protect the banking and finance infrastructure. The elected officials are considering making the regulatory agencies more accountable for the health and safety of the banking system. Their approach is to consolidate the regulatory agencies and implement strict codification of standards and procedures, with fewer regulations and regulators. Appointed officials who manage the regulatory system have a different solution — greater autonomy for examiners and less reshuffling and reorganization of authority and responsibility. The trade-off is between accountability and flexibility.

The U.S. banking regulatory structure is much like it was in 1950. The Federal Reserve, the Office of the Controller of the Currency, and the Federal Deposit Insurance Corporation have divided responsibilities for overseeing a rapidly changing and growing industry. Rather than stressing the need for training and experience in bank supervision, which would allow more flexibility in meeting the expected changes, the law now emphasizes across-the-board standards and strict adherence to regulations developed in response to the last banking crisis. One industry expert said that a trade-off occurs between strict political accountability and freedom of action in response to reforming the U.S. banking regulations.

The U.S. banking and finance infrastructure has evolved slowly. However, increased competition, new technology, and the amendment and revision of the law in the late 1990s have introduced substantial changes. The banking environment has moved from a fairly static, predictable industry to a dynamic, rapidly developing new structure. The regulatory scheme in 1975 probably will not be evident in 2000.

Although federal agencies continue to have the same compartmentalized responsibilities, dramatic changes probably will be made, as it becomes obvious that this structure may not be responsive and flexible enough to cope with the rate of change expected in the next two decades. Regulators must be free to apply different approaches to supervision and regulation, as appropriate, for a defined set of facts concerning a specific banking activity or bank. They must not be hampered by either bureaucratic intransigence or political expediency.

Rationale for Research and Desired Results

Open standards for the information infrastructure are important for interoperability and free-market competition. Rather than relying on many sources to develop software elements, banks and their customers increasingly depend on a handful of software suppliers — a new vulnerability that can affect the infrastructure. Government encouragement and support for open standards can strengthen the free-market environment and help to provide an infrastructure that is not constrained by a few entities.

Timeframe and Resource Requirements

In the near term (before 2002), research would focus on developing and publishing standards and specifications for the infrastructure. Funding required for these efforts is estimated to be $6 million.

3.2.6 Information Security Support for Electronic Commerce

Description

The U.S. financial payments architecture needs to be redesigned to support the national interests with respect to new international exchange environments and technologies. The technical options available for use by government, industry, and individual consumers need to be evaluated on the basis of their ability to support the security requirements yet to be defined for this infrastructure. The National Institute of Science and Technology and the National Security Agency have performed Underwriters Laboratory functions for these technologies on the basis of their potential impact on the surety of the banking and finance infrastructure. This arrangement should be fostered and enhanced.

Goals and Challenges

To remain competitive, the U.S. banking and finance infrastructure must be able to access cryptographic and surety technologies sufficient to maintain efficiency and effectiveness in protecting its customers' interests. These needs must be balanced against other national security interests.

Rationale for Research and Desired Results

The appropriate level of cryptographic technologies used in commercial applications must addressed immediately if the United States is to continue to be an economic world leader. International electronic commerce increases requirements for the robustness and surety of authentication mechanisms, for information systems and data integrity, and for innovative solutions to the trade-offs in balancing privacy and nonrepudiation. To support authentication requirements, biometric research needs to continue. Research also is needed to consider the applications of existing and developing technologies to satisfy more stringent requirements in infrastructure surety. Standards for integrating these technologies into system design should be developed as an incentive for industry to fill any gaps.

Timeframe and Resource Requirements

In the near term (before 2002), research would focus on publishing initial standards and specifications for equipment and support tools for the banking and finance infrastructure. Funding required for these efforts is estimated to be $9 million. Before 2005, researchers would field the standards and specifications. Funding required for these efforts is estimated to be $9 million. Before 2010, operational tools would be tested in the field. Funding required for these activities is estimated to be $3 million.

3.3 Technology R&D Shortfalls

Current commercial technologies may or may not be sufficient to protect the banking and finance infrastructure in the future. Various commercial off-the-shelf and government off-the-shelf products have been developed to provide security to financial information systems. However, most of these products lack the robustness and scaleability to secure our nation's information economy.

In addition, it is not clear that the private sector has the necessary motivation or incentive to develop the level of services that may be required to protect the infrastructure at the national level. Most private-sector parties work to capture market share or some other competitive advantage through their information technology innovations. Therefore, it is unlikely that the private sector would develop the open, scalable, and robust information technologies needed to foster a widespread competitive information economy.

Although the private sector apparently lacks sufficient incentive for developing certain technologies of importance to our national security, private/public-sector partnerships can play an active role in developing the necessary technologies. Areas in which partnerships are needed to help the banking and finance infrastructure to reach its full potential are described below.

3.3.1 Modeling and Simulation

It is unlikely that a single entity in industry can develop, maintain, and elaborate a scalable, flexible, and comprehensive constructive model of the entire banking and finance infrastructure because of the costs and complexities of such an enterprise. Industrial entities have few incentives for sharing information about their operations and structures. An industry/government consortium could develop such incentives; however, sufficient guarantees would have to be in place to protect proprietary business information. Moreover, the intent would have to be clear that the model and information would be used solely for analyzing technologies, making business arrangements, and developing regulatory schemes. These tasks would be directed at enabling the banking and finance infrastructure to move forward, not for surveillance or taxation of industry.

3.3.2 Key Management Systems

Cryptography plays a prominent role in most information security technologies. However, cryptographic methods are difficult, if not impossible, to implement without efficient, scalable mechanisms for managing key components. In particular, the banking and finance infrastructure of the future needs standard, open mechanisms for certifying public keys and cryptographic credentials. The industry must have access to better tools for evaluating cryptographic systems and have a well-defined method for comparing the appropriateness of such systems for specific applications.

3.3.3 Authentication Technologies

Our future information economy cannot reach its potential until science and industry develop better techniques for identifying and authenticating individuals and entities to information systems. The industry needs inexpensive, reliable, and scalable techniques to support the vast number of individuals who present themselves to information terminals or appliances for many reasons. Biometric identification techniques must be developed to meet these needs. Researchers also must concentrate on developing better sensors that can become as common as keyboards and touch-pads are today.

3.3.4 Intrusion and Anomaly Detection Tools

Tools that combine automated pattern recognition, sensitivity analysis, and nonlinear correlations are desperately needed to aid in deciding when an event is a systemic anomaly as opposed to when it is evidence of intentional malfeasance. It is unlikely that the banking and finance infrastructure could justify the necessary R&D as a

purely private matter; it would require a strong government support program. The need for such tools is not unique to this infrastructure, and the specification for, and costs of, such research, therefore, should not be borne solely by this infrastructure.

3.3.5 Computer and Network Security

All applicable technology areas depend significantly on research on computer and network security. Details of R&D requirements in security (Tab C, *Preliminary Research and Development Roadmap for Protecting and Assuring the Information and Communications Infrastructure)* should be reviewed for specific interdependencies with the banking and finance infrastructure. Any technologies that affect the robustness of the communications and computation systems that support banking and finance have a critical effect on this industry.

3.3.6 Physical and Electronic Protection Technologies

It is difficult to imagine that citizens and commercial entities would welcome an open electronic banking and finance infrastructure if the community had to rely on current technologies for protecting data stored in information systems. In particular, the community needs better techniques for keeping sensitive data safe from exposure, even when the same parties want to use open public networks and standard computing platforms for managing these data. Research is needed into highly secure, portable data storage, such as smartcards, cryptographic storage, and security-enhanced memories for microcomputers.

3.3.7 Electronic Payment Systems

The banking and finance infrastructure could make the transition from current concepts of electronic cash — and other unique tokens that can be converted to real currency — to the concept of electronic cash minted by the U.S. government. Electronic cash would provide the same full trusts and guarantees as physical currency carries today. Meanwhile, however, the industry needs payment mechanisms that enable an orderly transition from physical instruments to high-confidence electronic instruments, such as electronic checks and other widely accepted standard electronic payment mechanisms.

3.3.8 Network Security Management Systems

Finally, these technologies are not useful until they can be integrated into transaction support systems that are as available and robust as we have come to expect. Tomorrow’s technologies must be integrated so that they enhance the trust placed in today’s banking system.

3.4 R&D Topics and Roadmaps

In meeting its responsibilities, the government must combine patience with aggressive fact finding, study, and coordination among government units, both nationally and internationally. Premature action by government agencies, or decisions based on incomplete analysis, could "thwart innovation and its benefits, including, perhaps, the ability of U.S. firms to compete effectively in global markets" (U.S. Department of the Treasury 1996).

To protect national interests in an economic infrastructure characterized by international electronic commerce, the government must understand the existing infrastructure and its implications. These implications include its vulnerabilities and the changes in threat profiles that can develop as electronic commerce emerges. Table A.1 provides a summary description of the research topics and their interrelationships. This table summarizes programmatic expenditures for certain timeframes to address the vital issues raised above. The necessary R&D is grouped into clusters of technically related topics.

Table A.1 Summary of Banking and Finance R&D Topics[a]

Research Topic					
No.	Title (Type[b])	Product	Goals and Challenges	Threats and Vulnerabilities	Priority Category
1	Simulation Model Development[c] (A, ATD, POP)				
1.1	Specify and collect the minimal data set needed to describe the infrastructure. Develop a constructive strategic simulation of this infrastructure.	Scalable, constructive models capable of supporting useful simulations	Specify and collect data. Specify and characterize functional flow on how to engage the industry, protect information, determine inter-dependencies, identify available data and what is needed, and identify available and appropriate modeling techniques.	Complexities, inter-dependencies	Most important
1.2	Create, develop, and evaluate a process for engaging industry in developing, designing, and maintaining a constructive strategic simulation model (CSSM) for the U.S. government and banking and finance stakeholders.	Concept/strategy paper: process, set of recommendations (validated in industry forum), and an implementation plan	Determine the uses for the model. Define CSSM requirements, including interdependencies. Determine the architecture of the CSSM, especially protection of information.		
1.3	Develop the requirements, policies, legal basis, and techniques for protecting sensitive, proprietary, and classified data required for the CSSM (e.g., leverage existing work, models, mechanisms). Phase 1 involves historical and contemporary research. Phase 2 identifies gaps for making recommendations. Phase 3 gives iterations of Phase 2 during model development.	End-to-end model of the banking and finance infrastructure that can support nondeterministic simulations	Define required data. Identify available data and gaps. Determine available techniques/tools and gaps. Develop prototype CSSM. Test, validate, and develop life-cycle management methodology. Ensure that all developments are accurate, efficient, respond rapidly, and are timely.		
1.4	Specify, design, and code the CSSM.				
2	Information Security Analysis (A, ATD, POP)				
2.1	Analyze and evaluate the degree to which national strategic interests are adequately addressed by current cryptographic and surety analysis technologies, policies, and practices. If the answer reveals gaps, continue with topics 2.2–2.7.	Policy paper, including both legislative and procedural recommendations; information, hardware, and software	Find an independent, yet sufficiently knowledgeable team to do a reasonable analysis, given that full data for analyzing the problem might require sensitive and classified information. Acknowledge that this topic is a political "hot potato;" the intelligence agencies might object to this analysis. If gaps are found, making recommendations will be difficult, because it requires dealing with "equities" in National Security goals.	Cyber, complexities, inter-dependencies	Most important

Table A.1 (Cont.)

Research Topic					
No.	Title (Type[b])	Product	Goals and Challenges	Threats and Vulnerabilities	Priority Category
2.2	Develop a legal and procedural basis for expediting access to government off-the-shelf cryptographic analysis and surety analysis technology.	Development guidelines, metrics for judging the effectiveness of implementations, analysis techniques, and methodologies	Develop the means to allow effective and efficient analysis metrics to assure sound information system processing of banking and finance data with the appropriate level of security.		
2.3	Analyze and evaluate the efficacy of implementations of cryptographic and surety technologies.		Avoid the pitfalls from the "Rainbow Series" security guidelines in which evaluation processes cause unacceptable product cycle times. Include much more than algorithmic standards; allow judgment of the actual implementations of the systems. Support variable security levels required for variable data sensitivity.		
2.4	Develop and validate security implementation standards for banking and finance information applications (scalable, supporting variable security levels).		Note that the InfoSec community has struggled with variable security levels before, and it is not easy. Need to focus on the real requirements of the banking and finance infrastructure and find solutions that are much more efficient than those in place for defense applications today.		
2.5	Develop scalable public key management systems that are (a) applicable and usable for local, small-scale, and global banking and finance infrastructure; (b) capable of operating with other key management systems implemented for the information and communications infrastructure (the banking and finance community will rely on these systems); and (c) be useful and usable today and in the future.	Improved public management systems with listed properties. Policy papers and recommendations for handling liabilities if any key management systems fail. Specifications and designs for better entity identification technologies.	Keep in mind that all developers of standards have traditionally been very slow in taking actions. Develop effective public management systems for information security applications that process banking and finance data. Avoid developing many noninteroperating certificate authorities that make assured operations risky. Look at scaleability of solutions – both large and small systems. Assign liabilities involved in potential failures in certificate authorities.		

Table A.1 (Cont.)

Research Topic No.	Research Topic Title (Type[b])	Product	Goals and Challenges	Threats and Vulnerabilities	Priority Category
			(Many are developing certificate authority systems, although not all are suitable for the banking and finance infrastructure. The industry is investing in the area, but federal dollars might ensure interoperability and better security features in most systems. This is why the dollar amount is relatively small. [Work in key recovery will be a part of this, but other R&D efforts are important.])		
2.6	Develop more effective ways to authenticate entities – persons and systems – that use the banking and finance infrastructure. Improve "biometric" identity systems for individuals – strongly linked to physical tokens that represent these individuals in a system. Develop mechanisms for authenticating authorized users of the equipment in systems.	Position paper evaluated by the stakeholders on the policy of the U.S. banking and finance infrastructure with respect to this issue. Recommendations for required legislation to cover this policy. Prototypical solutions that provide a balance of technical support.	Develop better, cost-effective biometric systems. Be more careful in linking biometrics of the individual to the physical token used by systems to identify individuals. Implement stronger methods for verifying that certain equipment used in remote systems has not been modified in an unauthorized manner. Find cost-efficient methods to identify unauthorized changes to equipment.		
2.7	Clarify and resolve to achieve an appropriate balance between the need for anonymity and nonrepudiation in information security systems for the banking and finance infrastructure.		Analyze the issues involved. Develop cryptographic and system solutions for balancing competing issues. Develop legislative actions to support these solutions.		
3	Intrusion Indication and Warning (I&W) Tools (B, A, ATD, POP)				
3.1	Determine where I&W tools and techniques are applicable	Information, hardware, software	Aim for accuracy, efficiency, and rapid response time.	Cyber, inter-dependencies	Very important
3.2	Develop a suite of intrusion and anomaly detection tools.				
3.3	Develop suite of technology sensitivity analysis tools.				
4	Systems Reliability Enhancement (B, A, ATD, POP)				
4.1	Develop standards for high-availability/high-reliability systems	Information, hardware, software	Understand the environment.	Complexities, inter-dependencies	Very important

Table A.1 (Cont.)

Research Topic					
No.	**Title (Type[b])**	**Product**	**Goals and Challenges**	**Threats and Vulnerabilities**	**Priority Category**
4.2	Develop standards for dynamically configurable firewalls.				
4.3	Analyze the utility and efficiency of network agent defenses.				
4.4	Develop standards for self-healing systems.				
5	Information System Standardization (A)	Information, policy, documents	Determine how to engage the industry.	Complexities, inter-dependencies	Important
6	Electronic Commerce Security Enhancement (B, A, ATD, POP)	Information, hardware, software.	Understand the environment. Determine how to engage the industry.	Complexities, inter-dependencies	Important
6.1	Develop standards for user equipment and network security				
6.2	Implement authentication tools and techniques. (7 years, $15 million)				

[a] The order of the R&D topics within a priority category (i.e., most important, very important, important) does not imply relative importance. Some of these tasks must be done in parallel - some are iterative.

[b] B = basic; A = applied; ATD = advanced technology development; and POP = proof of principle and validation.

Section 4
R&D Topic Roadmaps

The suggested roadmap for each of the R&D topics identified and presented by the Banking and Finance R&D Roadmapping Team is summarized in Table A.2. The accomplishments during three phases of research (i.e., near term [before 2002], by approximately 2005, and by approximately 2010) are summarized. More detailed information can be found in Section 3, which contains more detailed topic descriptions.

Table A.2 Summary of the Banking and Finance Infrastructure R&D Roadmap

R&D Topic No.	R&D Topic Title	Near Term (Resource Estimate[a])	Achieved by ~2005 (Resource Estimates[a])	Achieved by ~2010 (Resource Estimate[a])
1	Simulation Model Development	Engage industry and design and develop a constructive strategic simulation model (CSSM). ($18 million)	Develop the requirements, legal basis, policies, and techniques for protecting the sensitive, proprietary, and classified data required for the CSSM. Leverage existing work, models, mechanisms, etc. ($10 million)	Prepare field operational model and life-cycle management plan. ($1 million)
2	Information Security Analysis	Develop a legal and procedural basis for expediting access to government off-the-shelf cryptographic analysis and surety analysis technology. Analyze and evaluate the efficacy of implementations of cryptographic and surety technologies. Develop and validate security implementation standards for banking and finance information applications (scalable, supporting variable security levels). ($32 million)	Implement anonymity balance. Field scalable key public management systems. ($6 million)	Field entity authentication technologies. ($1 million)
3	Intrusion Indication and Warning (I&W) Tools	Use insight from the development of the CSSM to determine where within the system I&W and sensitivity tools and techniques are applicable. Determine what data are required to implement those tools and techniques. ($29 million)	Develop an initial suite of tools. ($7 million)	Field operational tools. ($1 million)
4	Systems Reliability Enhancement	Develop, publish, and begin to implement initial standards and specifications. Develop prototypes of network security agents. ($54 million)	Complete implementation of standards and specifications, and prototypes of network security agents. ($15 million)	Field prototypes of self-healing systems, configurable firewalls, and network defense agents. ($2 million)
5	Information System Standardization	Publish initial standards for open architecture. ($6 million)		
6	Electronic Commerce Security Enhancement	Publish initial standards and specifications for equipment and support tools. ($9 million)	Field standards. ($9 million)	Field operational tools. ($3 million)

[a] Resource estimates reflect qualitative, order-of-magnitude judgments. They are intended to be representative of the resources needed for the R&D topics and are based on assumptions concerning the scope, the expected level of effort, and the pace of the research. Detailed cost estimates must be prepared in concert with the development of detailed R&D plans.

Section 5
References

Booz-Allen and Hamilton, Inc., 1996, "Executive Summary — U.S. Banking and Finance Infrastructure Security Assessment."

Defense Science Board, 1996, Task Force on Information Warfare, Nov. (http://www.infowar.com).

General Accounting Office, 1996, *Information Security-Opportunities for Improved OMB Oversight of Agency Practices*, Washington, D.C., Sept.

Jones, E., and A. Sicherman, 1997, *Evaluating and Managing the Integrity of Computerized Accountability Systems Against Insider Threats*," Lawrence Livermore National Laboratory, Livermore, Calif.

Kennedy, J.T., 1998, "Internet Intricacies: Don't Get Caught in the Net," *Contingency Planning and Management* III(1):12–18, Jan.

Reno, J., 1998, speech presented by the U.S. Attorney General at Lawrence Livermore National Laboratory, Livermore, Calif., Feb. 25.

U.S. Department of the Treasury, 1993, *Future Trend Alert*, Nov.

U.S. Department of the Treasury, 1996, "An Introduction to Electronic Money Issues," *Toward Electronic Money and Banking: The Role of Government*, Conference held in Washington, D.C., September 19–20.

U.S. Senate, 1996, Permanent Subcommittee on Investigations, Hearings on Security in Cyberspace (Minority Staff Report), June 5.

Wriston, W., 1992, *The Twilight of Sovereignty*, Charles Scribner's & Sons, New York, N.Y.